PREMIÈRE
MINISTRE

Liberté
Égalité
Fraternité

Première ministre

Agence nationale de la sécurité des systèmes d'information

Référentiel d'exigences de sécurité pour les moyens d'identification électronique

Version 1.2. du 11 août 2022

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
19/04/2018	*1.0.b projet*	*Version pour commentaires*	ANSSI
29/08/2018	*1.0.d projet*	*Prise en compte des commentaires de la Direction Générale des Entreprises*	ANSSI
30/09/2021	*1.1*	*Version de référence pour l'attestation de conformité*	ANSSI
11/08/2022	*1.2*	*Mise à jour du référentiel pour prise en compte du décret d'application du L. 102 du CPCE et de la publication du référentiel d'exigences « PVID ».*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

supervision-eIDAS@ssi.gouv.fr

SOMMAIRE

I. Introduction

Note préliminaire relative à l'utilisation du présent document: celui-ci contient des références documentaires signalées par l'emploi de crochets []. La liste des références documentaires est disponible en annexe, en fin de ce document.

I.1. Objet

Le présent document spécifie les exigences de sécurité applicables pour la certification des moyens d'identification électronique délivrés dans le cadre de schémas d'identification électronique tels que définis par le règlement européen [eIDAS].

Ce document précise les exigences du règlement d'exécution (UE) 2015/1502 de la commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014.

I.2. Cadre juridique

L'article L. 102 du Code des postes et des communications électroniques introduit la certification par l'ANSSI des moyens d'identification électronique dont le présent document constitue le référentiel d'exigences. En particulier :

- Pour la certification des moyens d'identification électronique présumés fiables prévue au III de cet article L. 102, le cahier des charges mentionnés s'appuie sur les exigences pour le niveau de garantie élevé définies dans le présent document ;

- Pour la certification des moyens d'identification électronique autres que présumés fiables, le présent document constitue le référentiel d'exigence mentionné au IV de l'article L. 102.

Les moyens d'identification électronique ayant fait l'objet d'une certification de conformité par l'ANSSI aux exigences du niveau de garantie substantiel ou élevé, sont présumés satisfaire aux critères définis à l'article 8, paragraphe 2 du règlement [eIDAS], et aux exigences du règlement d'exécution [2015/1502] en vertu du paragraphe 3.

L'ANSSI ne délivre pas de certification pour les moyens d'identification électronique visant le niveau de garantie faible.

La fourniture de moyens d'identification électronique suppose un traitement de données à caractère personnel au sens de l'article 4-2 du [RGPD]. A ce titre, le fournisseur de moyen d'identification respecte, dès la conception du schéma d'identification électronique et par défaut, les principes essentiels en matière de protection des données à caractère personnel rappelés dans le présent référentiel et les exigences du [RGPD] et de la [LIL].

I.3. Processus de certification

L'évaluation de la conformité aux exigences du présent document repose sur plusieurs sous-processus :

- Un audit de l'organisme fournissant le moyen d'identification électronique ainsi que des partenaires et sous-traitants impliqués dans la fourniture de ce moyen, tel que décrit dans le présent document au chapitre II.2.4.7. Le présent document spécifie les caractéristiques de cet audit selon le niveau de garantie visé ;

- La qualification des moyens de cryptologie constitutifs du moyen d'identification électronique, tel que décrit dans le document [QUALIF_PROD]. Le présent document spécifie le niveau de qualification nécessaire et le caractère obligatoire ou recommandé de cette qualification, selon le cas ;

- Un audit spécifique, le cas échéant, des solutions mises en œuvre pour permettre la vérification d'identité à distance des demandeurs de moyens d'identification électronique, au regard des exigences du référentiel [PVID]. En cas de recours à un service certifié conforme au référentiel [PVID] par l'ANSSI ou par un organisme de certification qu'elle a autorisé, la conformité à ces exigences est présumée, pour le niveau de garantie couvert par la certification.

La demande de certification d'un moyen d'identification électronique est à adresser au Bureau Qualifications et Agréments de l'ANSSI (qualification@ssi.gouv.fr).

La demande peut être adressée par tout organisme souhaitant faire certifier un moyen d'identification électronique au titre de l'article L. 102 du Code des postes et des communications électroniques.

Cette certification est un prérequis à la notification d'un schéma d'identification électronique par l'État français dans le cadre du règlement [eIDAS].

Les modalités de certification par l'ANSSI sont précisées dans le document [CERT_SERV_PROCESS].

La division Industries et Technologies de l'ANSSI (industries@ssi.gouv.fr) est le point de contact privilégié pour toute question relative à la démarche de certification d'un nouveau dispositif.

I.4. Mise à jour

L'opportunité de la mise à jour de ce document est évaluée par l'ANSSI et peut être le fait d'une évolution du cadre réglementaire ou normatif, de l'état de l'art ou du processus de certification d'un moyen d'identification électronique.

Conformément au second alinéa de l'article R. 54-2 du Code des postes et des communications électroniques, la publication d'une nouvelle version de ce référentiel est assortie d'un préavis de trois mois avant son entrée en vigueur.

I.5. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DPI	*Dot Per Inch*
EAC	*Extended Access Control*
EAL	*Evaluation Assurance Level*
FIDO	*Fast IDentity Online*
HSM	*Hardware Security Module*
INSEE	Institut National de la Statistique et des Etudes Economiques
LCP	*Lightweight Certificate Policy*
LCR	Liste des Certificats Révoqués
MRZ	*Machine-Readable Zone*
NCP	*Normalized Certificate Policy*
OCSP	*Online Certificate Status Protocol*
OTP	*One-Time Password*
PACE	*Password Authenticated Connection Establishment*
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information
PIN	*Personal Identification Number*
PRADO	*Public Register of Authentic identity and travel Documents Online*
PVID	Prestataire de Vérification d'Identité à Distance
RGS	Référentiel Général de Sécurité
RNA	Répertoire National des Associations
TLS	*Transport Layer Security*
SIREN	Système Informatique pour le Répertoire des ENtreprises
SIRENE	Système Informatique pour le Répertoire des ENtreprises et des Etablissements
SIRET	Système Informatique pour le Répertoire des ETablissements
SMS	*Short Message Service*
TVA	Taxe sur la Valeur Ajoutée
USB	*Universal Serial Bus*
U2F	*Universal 2nd Factor*
VIES	*Value Added Tax (VAT) Information Exchange System*

II. Exigences relatives aux niveaux de garantie des moyens d'identification électronique

Note préliminaire relative à l'utilisation du présent chapitre: le contenu du règlement d'exécution [2015/1502] est repris en encadré bleu (le texte est repris en caractères normaux ; les aménagements rédactionnels pour la clarté du document en caractères *italiques*).

Par ailleurs, ce chapitre est émaillé d'exemples en caractères *italiques* – ces derniers ne sont ni normatifs, ni exclusifs, mais sont destinés à faciliter la compréhension des exigences.

La numérotation des titres de cette section suit celle du règlement d'exécution. *Par exemple, la section II.2.1.2 ci-dessous correspond à la section 2.1.2 du règlement d'exécution.*

II.1. Définitions applicables

Les définitions suivantes s'appliquent :

En complément des définitions listées dans le règlement [eIDAS] et dans le règlement d'exécution [2015/1502], les définitions suivantes sont utilisées dans le présent document :

- « demandeur » fait référence à une personne physique demandant un moyen d'identification électronique et dont l'identité doit être vérifiée ;

- « utilisateur » personne physique qui, pour s'identifier auprès d'un service numérique, utilise un moyen d'identification électronique ;

- « fournisseur de moyen d'identification électronique » fait référence à une personne morale, publique ou privée, délivrant au demandeur le moyen d'identification électronique.

Le « demandeur » devient « utilisateur » dès lors que les vérifications d'identité et la délivrance du moyen d'identification électronique ont été réalisées avec succès.

Dans le cadre d'une tutelle telle que définie aux articles 440 et suivants du code civil, le tuteur peut initier la démarche de demande de moyen d'identification électronique pour le compte de la personne qu'il a sous sa tutelle. Les termes « demandeur » et « utilisateur » dans les chapitres suivants s'appliquent, dans ce cas, à la personne sous tutelle.

Tout au long du règlement d'exécution [2015/1502] relatif aux niveaux de garantie et du présent référentiel, le terme « document » renvoie à un document sous forme physique ou sous forme électronique. Le terme « élément d'identification » renvoie à un élément d'identification sous forme physique ou sous forme électronique.

(1) « source faisant autorité » : toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité ;

Une source faisant autorité est une source, quelle qu'elle soit, considérée comme fiable au niveau national en ce qui concerne la fourniture de données valides. Une source ne peut faire autorité que pour les informations qu'elle fournit.

Lorsqu'une source faisant autorité est à l'origine d'éléments d'identification, les informations relatives à ces éléments d'identification peuvent être considérées comme représentant l'identité telle qu'elle est connue de la source faisant autorité au moment de la délivrance, à condition que l'authenticité et la validité de ces éléments d'identification puissent être confirmées (*Par exemple, le répertoire « Sirene » est à l'origine d'un extrait « K-bis ». Autre exemple, le passeport biométrique est à l'origine des données d'état civil lues depuis la puce électronique).*

Les sources faisant autorité diffèrent pour les personnes physiques et les personnes morales :

- Conformément à l'alinéa 4º de l'article R. 54-1 du Code des postes et des communications électroniques, sont reconnus comme sources faisant autorité pour la preuve et la vérification d'identité des personnes physiques lors de la délivrance d'un moyen d'identification électronique :

    - pour les Français, les ressortissants des autres États membres de l'Union européenne, d'un État partie à l'accord sur l'Espace économique européen ou de la Suisse, le passeport ou la carte nationale d'identité ;
    - pour les ressortissants de pays tiers résidant en France ou dans un autre État membre de l'Union européenne, dans un État partie à l'accord sur l'Espace économique européen ou en Suisse, le titre de séjour, établi selon le modèle prévu par le règlement (UE) nº 2017/1954 du parlement européen et du conseil du 25 octobre 2017 modifiant le règlement (CE) nº 1030/2002 du Conseil établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, délivré par l'État de résidence ;
    - pour les ressortissants de pays tiers dispensés de l'obligation de visa de court séjour ne résidant pas sur le territoire de l'Union européenne, dans un État partie à l'accord sur l'Espace économique européen ou en Suisse, le passeport, sous réserve que le pays émetteur mette à disposition les moyens nécessaires à la vérification de la validité du titre. Si la dispense de l'obligation de visa est assortie de l'obligation de disposer d'un passeport électronique, seul le passeport biométrique est reconnu comme source faisant autorité pour le pays concerné ;
    - pour les ressortissants de pays tiers réfugiés ou reconnus apatrides ou bénéficiaires de la protection prévue par la directive 2011/95/UE du Parlement européen et du Conseil du 13 décembre 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale, à un statut uniforme pour les réfugiés ou les personnes pouvant bénéficier de la protection subsidiaire, et au contenu de cette protection, le passeport est remplacé par le titre de voyage délivré par l'État qui a reconnu la qualité de réfugié ou d'apatride ou accordé la protection.

Ces sources faisant autorité sont considérées comme valides si elles n'ont pas atteint leur date de fin de validité et n'ont pas fait l'objet d'une invalidation.

- Sont reconnus comme sources faisant autorité pour la preuve et la vérification d'identité des personnes morales établies en France :

- le Système national d'identification et du répertoire des entreprises et de leurs établissements (« répertoire Sirene ») maintenu par l'Institut national de la statistique et des études économiques (« Insee ») ;
- le répertoire national des associations (RNA) ;
- le Journal officiel de la République française portant création d'une association ;
- le Journal officiel de la République française portant création et définissant les missions d'une administration ;
- le registre des associations tenu par le tribunal d'instance pour les départements de Moselle, Bas Rhin et Haut Rhin.

Pour les personnes morales établies hors de France, le système VIES de la Commission européenne est une source faisant autorité permettant de confirmer la validité d'un numéro de TVA intra-communautaire.

(2) « facteur d'authentification » : un facteur confirmé comme étant lié à une personne, qui relève de l'une des catégories suivantes :

Les facteurs d'authentification peuvent être répartis dans les catégories suivantes, chacune étant détaillée ci-après :

- facteurs d'authentification basés sur la possession (ce que l'on possède, *par exemple, une carte à puce*) ;
- facteurs d'authentification basés sur la connaissance (ce que l'on sait, *par exemple, un mot de passe ou un code PIN*) ;
- facteurs d'authentification inhérents (ce que l'on est, *par exemple, une empreinte digitale ou une photographie*).

Le ou les facteur(s) d'authentification peuvent être utilisés soit directement (*par exemple, saisie d'un mot de passe*), soit indirectement afin de déverrouiller un dispositif qui fournira ensuite l'authentification (*par exemple, envoi d'une preuve de possession d'une clé privée*).

Des facteurs d'authentification relevant de différentes catégories peuvent également être combinés. Un moyen d'identification électronique qui utilise plusieurs facteurs relevant de différentes catégories est qualifié de multifactoriel, *par exemple : une carte à puce (possession) activée au moyen d'un code PIN (connaissance)*.

Lorsqu'une authentification multifactorielle est utilisée, les différents facteurs doivent être choisis de façon à se protéger des attaques applicables au mécanisme d'authentification.

(a) « facteur d'authentification basé sur la possession » : facteur d'authentification dont il revient au sujet de démontrer la possession ;

Les principales caractéristiques de sécurité d'un facteur d'authentification basé sur la possession sont son contrôle exclusif par son propriétaire et la facilité d'utilisation de mécanisme d'authentification robuste. Il est, en outre, essentiel que sa reproduction ou falsification par un tiers soit rendue aussi difficile que possible et qu'elle soit facilement détectable. Le niveau de garantie

dépend du niveau de résistance à la fraude et à la contrefaçon. *Un facteur basé sur la possession peut être par exemple une carte à puce ou un dispositif USB contenant une clé privée, la carte SIM d'un téléphone mobile comportant des données d'identification, ou un dispositif matériel permettant de générer des codes à usage unique (« OTP »).*

Les attaques typiques perpétrées contre les facteurs d'authentification basés sur la possession sont le vol, la duplication, l'altération ou la falsification, ainsi que les attaques perpétrées lors de l'authentification au moment d'établir la preuve de la possession. Lors de l'emploi de codes à usage unique, les attaques peuvent également concerner leur transmission ou leur affichage.

(b) « facteurs d'authentification basés sur la connaissance » : facteur d'authentification dont il revient au sujet de démontrer la connaissance ;

Un facteur d'authentification basé sur la connaissance est en principe connu du seul propriétaire du facteur et de l'entité chargée de vérifier l'authenticité des informations transmises, *par exemple : code PIN, mot de passe ou autre information que seul l'utilisateur est susceptible de connaître*. Il se peut que cette entité elle-même ne connaisse pas l'exact facteur d'authentification basé sur la connaissance, mais soit en mesure de confirmer qu'elle et le demandeur connaissent exactement la même information, *par exemple en vérifiant l'empreinte d'un mot de passe*.

Si la connaissance d'un secret est utilisée comme un facteur, il convient de limiter les risques qu'un adversaire devine (au hasard ou par force brute) celui-ci. *Par exemple, lorsque le facteur d'authentification est un mot de passe, les bonnes pratiques recommandent une politique appropriée en matière de mots de passe (voir les notes [SECU_MDP] et [RGS_B3]).*

Les attaques typiques perpétrées contre les facteurs d'authentification basés sur la connaissance sont la déduction, l'hameçonnage, l'écoute ou le rejeu. L'une des caractéristiques des facteurs d'authentification basés sur la connaissance est que les attaques dont ils font l'objet ne sont pas nécessairement détectées par l'utilisateur du moyen d'identification électronique. *C'est le cas, par exemple, des attaques par force brute ou par dictionnaire dirigées contre un mot de passe à faible entropie et ne disposant pas d'un système de limitation des essais, ou contre un mot de passe qui a été recopié à partir d'une lettre ou d'un courriel sans que l'utilisateur ne le sache.*

(c) « facteur d'authentification inhérent » : un facteur d'authentification qui est basé sur un attribut physique d'une personne physique, et dont il revient au sujet de démontrer qu'il possède cet attribut physique ;

Les facteurs d'authentification inhérents (ou facteurs biométriques) doivent être différents d'une personne physique à l'autre, y compris lorsque des personnes physiques présentent des caractéristiques similaires, de sorte qu'une personne physique puisse être identifiée de façon unique, *par exemple, les empreintes digitales, les empreintes palmaires, la forme du visage, la géométrie de la main, la forme de l'iris ou la voix.*

Un élément déterminant lié à l'utilisation de facteurs biométriques est de garantir la présence physique sur le lieu de la vérification de la personne physique à laquelle ils correspondent. Le niveau de garantie dépendra de la résistance aux attaques visant à usurper l'identité de la personne physique en leurrant le mécanisme de reconnaissance biométrique (*par exemple, via la présentation d'une photographie ou d'une séquence vidéo préenregistrée ou altérée, ou d'un moulage de l'empreinte digitale de la personne physique*). L'emploi de technologies de détection du vivant permet de renforcer cette résistance.

(3) « authentification dynamique » : un processus électronique utilisant la cryptographie ou d'autres techniques pour fournir un moyen permettant de créer sur demande une preuve électronique attestant que le sujet contrôle ou possède les données d'identification et qui change avec chaque authentification entre le sujet et le système vérifiant l'identité du sujet ;

L'objectif principal de l'authentification dynamique est de limiter les risques d'attaques telles que les attaques de type « homme du milieu » ou les attaques reposant sur le rejeu d'une authentification préalablement enregistrée. Cela inclut, sans être exhaustif :

- les attaques par rejeu, autrement dit, le fait d'intercepter des données d'authentification et de les réutiliser dans un contexte d'authentification différent ;

- certains types de détournements de session, par exemple l'échange des contextes d'authentification de plusieurs authentifications survenant simultanément.

L'authentification multifactorielle et l'authentification dynamique ne sont pas équivalentes ; une authentification multifactorielle n'implique pas que l'authentification soit dynamique et peut par conséquent être davantage exposée aux attaques par rejeu qu'une authentification dynamique.

L'authentification dynamique peut être mise en œuvre par le facteur d'authentification (*par exemple, une clé à usage unique issue d'un dispositif cryptographique*) ou par le mécanisme d'authentification (*par exemple, un défi dynamique dans une authentification par défi-réponse*).

Parmi les exemples de mécanismes d'authentification dynamique figurent :

- *la mise en œuvre d'une clé privée stockée sur un moyen de cryptologie matériel sécurisé et sous le contrôle exclusif de l'utilisateur dans le cadre d'un protocole défi-réponse ;*

- *l'emploi de protocoles s'appuyant sur un échange de clés Diffie-Hellman éphémères et fournissant une authentification (par exemple, PACE), sur des nonces cryptographiques, sur des horodatages ou sur des numéros séquentiels non répétés ;*

- *l'emploi de protocoles basés sur un échange de clés Diffie-Hellman éphémère-statique, si la clé éphémère est fournie par la partie utilisatrice (par exemple, EAC) ;*

- *l'utilisation de codes d'accès à usage unique générés de façon dynamique (par exemple, des authentifications s'appuyant sur un OTP) ;*

(4) « système de gestion de la sécurité de l'information » : un ensemble de processus et de procédures visant à gérer les risques associés à la sécurité de l'information pour les maintenir à des niveaux acceptables ;

La norme [ISO_27001] référence les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de gestion de la sécurité de l'information.

Si le moyen d'identification électronique repose sur l'emploi de certificats électroniques, la norme [EN_319_411-1] spécifie les bonnes pratiques relatives à la délivrance et la gestion du cycle de vie des certificats électroniques.

II.2. Spécifications techniques et procédures

Les éléments des spécifications techniques et des procédures décrits dans la présente annexe servent à déterminer de quelle façon les exigences et les critères de l'article 8 du règlement (UE) nº 910/2014 sont appliqués aux moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique.

Les exigences visées aux sections 2.1 et 2.2 de l'annexe du règlement d'exécution [2015/1502] font référence aux exigences relatives au processus « d'inscription » et de « gestion des moyens d'identification électronique », dont la « délivrance ». Il s'agit d'exigences fonctionnelles qui doivent être satisfaites au plus tard au moment de la première utilisation du moyen d'identification électronique.

II.2.1. Inscription

Le règlement d'exécution [2015/1502] utilise le terme « inscription » pour désigner le processus complet se déroulant en plusieurs étapes détaillées dans les points suivants :

- demande et enregistrement (chapitre II.2.1.1) ;
- preuve et vérification d'identité (chapitre II.2.1.2 pour les personnes physiques, II.2.1.3 pour les personnes morales et II.2.1.4 pour le lien établi entre les moyens d'identification électronique de personnes physiques et personnes morales).

II.2.1.1. Demande et enregistrement

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

1. S'assurer que le demandeur est informé des conditions associées à l'utilisation du moyen d'identification électronique.

2. S'assurer que le demandeur est informé des précautions de sécurité recommandées relatives au moyen d'identification électronique.

Les termes et conditions d'utilisation du moyen d'identification électronique, incluant toute limitation de responsabilité du fournisseur de moyen d'identification électronique, et précisant l'ensemble des précautions de sécurité recommandées, doivent être formalisés dans des conditions générales d'utilisation. Ces conditions générales d'utilisation doivent faire l'objet d'une acceptation explicite par le demandeur.

Exemples de précautions de sécurité :

- *choisir un mot de passe ou un code PIN sécurisé conformément à la politique communiquée ;*
- *stocker de manière sécurisée les moyens d'identification électronique basés sur la possession ;*

- *ne pas communiquer ses moyens d'identification électronique à un tiers.*

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

3. Recueillir les données d'identité pertinentes requises pour la preuve et la vérification d'identité.

Les données d'identité minimales qui seront transmises à chaque identification électronique de la personne (telles que définies dans le règlement d'exécution [2015/1501], notamment nom de famille tel qu'il résulte de l'acte de naissance, nom d'usage le cas échéant, prénoms, sexe, date et lieu de naissance) doivent être recueillies.

Le traitement des données à caractère personnel, et plus particulièrement pour des données dites « sensibles », est effectué en application du règlement [RGPD]. Le demandeur doit être informé des traitements réalisés sur les données recueillies conformément aux articles 13 et 14 du [RGPD]. Si un traitement de données biométriques du demandeur est réalisé, il doit être justifié par le respect de l'une des conditions prévues à l'article 9.2 du [RGPD].

La collecte de données autres que celles mentionnées dans le présent document est limitée au strict nécessaire au regard de la finalité du traitement permettant la délivrance du moyen d'identification électronique.

Dans le cas où le traitement réalisé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, une analyse d'impact sur la protection des données à caractère personnel (« AIPD ») doit être réalisée. Cette AIPD doit être transmise à la CNIL s'il persiste un risque résiduel élevé.

II.2.1.2. Preuve et vérification d'identité (personne physique)

Dans le cadre de la tutelle, et lorsqu'il a connaissance de cette situation, le fournisseur de moyen d'identification électronique prend en compte ces spécificités lors de la vérification d'identité :

- 1) Dans le cadre où le tuteur réalise la demande pour le compte de la personne sous tutelle, le fournisseur de moyen d'identification électronique contrôle, en plus de l'identité de la personne sous tutelle, l'identité du tuteur ainsi que le dernier jugement de tutelle ;

- 2) Dans le cadre où la personne sous tutelle réalise elle-même la demande, le fournisseur de moyen d'identification électronique contrôle l'attestation du tuteur indiquant qu'il est informé de la démarche, la photocopie de la pièce d'identité du tuteur, ainsi que le dernier jugement de tutelle.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

1. La personne peut raisonnablement être présumée en possession d'un élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et représentant l'identité alléguée.

Les éléments d'identification reconnus en France sont obtenus en s'appuyant sur les documents d'identité reconnus comme sources faisant autorité, référencés au chapitre II.1 du présent document.

Exemple : la présomption de possession peut être assurée par la présentation d'une copie du document d'identité sous forme physique ou électronique.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

2. L'élément d'identification peut être présumé authentique ou on peut présumer qu'il existe selon une source faisant autorité et cet élément semble être valide.

Le terme « authentique » fait référence à l'authenticité de l'élément d'identification au moment de la délivrance. On peut présumer qu'il demeure authentique s'il n'a pas été falsifié ou contrefait et s'il provient d'une source faisant autorité.

Le terme « validité » fait référence à l'exactitude de l'élément d'identification au moment de sa présentation.

Cela concerne, entre autres, l'exactitude des informations d'un document d'identité et son statut (déclaré perdu ou volé, expiré, ou valide).

Pour les documents d'identité reconnus comme sources faisant autorité recensés au chapitre II.1 du présent document, la vérification doit permettre d'établir que :

- l'ensemble des données d'identité nécessaires à l'inscription sont lisibles et conformes aux données transmises dans la demande ;

- le document d'identité est en cours de validité ;

- le document d'identité présenté n'a pas fait l'objet d'une falsification ou contrefaçon évidente, *par exemple le document ne comporte pas d'anomalies telles que des fautes d'orthographe, des polices visiblement différentes, des pages manquantes ou des incohérences flagrantes dans sa mise en page et son alignement, et la photographie présente sur le document ne paraît pas avoir altérée*.

Exemples :

- *La vérification de l'authenticité des documents d'identité physiques peut se faire par lecture des informations disponibles (visibles et/ou lisibles par un humain ou par des équipements optoélectroniques) sur l'élément physique ou sur une copie transmise par voie électronique ;*

- *En ce qui concerne les éléments d'identification lus par voie électronique, la vérification des signatures numériques apposées par l'autorité délivrant l'élément constitue le cas échéant une bonne pratique pour vérifier l'authenticité des données*.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

3. L’existence de l’identité alléguée est connue d’une source faisant autorité et on peut présumer que la personne est bien celle qu’elle prétend être.

On entend par identité alléguée, l’identité revendiquée par le demandeur du moyen d’identification électronique et constituée par les éléments d’identification présentés.

Le terme « existence » sous-entend notamment que la personne physique représentée par l’identité alléguée n’est pas décédée.

Afin de prouver que le demandeur est bien la personne physique qu’elle prétend être, une comparaison physique, par exemple par rapport à la photographie ou à la signature manuscrite portées par le document d’identité, peut être effectuée.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

Niveau faible, plus l’une des options énumérées aux points 1 à 4 ci-après :

1. Il a été vérifié que la personne est en possession d’un élément d’identification reconnu par l’État membre dans lequel est déposée la demande relative au moyen d’identification électronique et représentant l’identité alléguée

et

l'élément d’identification fait l’objet d’une vérification visant à déterminer son authenticité ou l’existence de cet élément est connue d’une source faisant autorité et il se rapporte à une personne réelle

et

des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification ;

ou

2. Une pièce d'identité est présentée au cours d'un processus d'enregistrement dans l'État membre où la pièce d'identité a été délivrée et la pièce d'identité semble se rapporter à la personne qui la présente

et

des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de la pièce d'identité ;

En France, ces deux cas sont traités de manière similaire, puisque les documents d’identité listés au chapitre II.1 du présent document sont reconnus comme sources faisant autorité.

La vérification d’identité doit permettre de vérifier que les caractéristiques physiques du demandeur correspondent aux informations provenant de la source faisant autorité. *Par exemple*

en vérifiant la correspondance entre le visage de la personne et la photographie portée sur le document d'identité. Cette vérification permet de minimiser les risques liés à la perte ou au vol de document.

En complément de la vérification de correspondance entre le demandeur et le document d'identité présenté, il est nécessaire de vérifier l'authenticité du document d'identité.

Le présent document distingue trois cas pour cette vérification d'authenticité, détaillés ci-après.

Cas de la vérification d'authenticité d'un document d'identité présenté lors d'un face à face physique

La vérification de l'authenticité d'un document d'identité présenté lors d'un face-à-face physique se fait au moyen d'une inspection des caractéristiques de sécurité du document d'identité. *Parmi les exemples de caractéristiques de sécurité figurent les filigranes, les encres, les hologrammes, et la micro-impression.*

Le registre en ligne de documents authentiques d'identité et de voyage PRADO, disponible sur le site internet du conseil de l'Union européenne www.consilium.europa.eu/prado/fr, et alimenté par les Etats membres, recense les caractéristiques de sécurité des documents d'identité.

Au niveau de garantie substantiel, le personnel inspectant des documents d'identité doit :

- avoir reçu une formation à la détection des documents falsifiés basée sur des supports pédagogiques de qualité ;

- être capable d'identifier des documents falsifiés/contrefaits.

Si un État met à disposition un service en ligne permettant d'identifier les documents déclarés perdus ou volés par leur détenteur, ce service doit être utilisé. Dans le cas contraire, les mécanismes mis en œuvre de vérification d'authenticité du document et de vérification d'identité du demandeur doivent permettre de se prémunir efficacement des risques liés à l'utilisation de documents perdus ou volés.

Cas de la vérification d'authenticité d'un document d'identité sur la base d'une photocopie ou d'une image numérisée

La vérification d'authenticité d'un document d'identité sur la base d'une photocopie ou d'une image numérisée ne peut être considérée comme une méthode suffisante que dans l'un ou l'autre des deux cas suivants :

- 1) La réalisation de la photocopie ou de l'image numérisée est réalisée dans les conditions cumulatives suivantes :

    - Elle est réalisée dans un guichet, sous le contrôle d'un membre du personnel de l'entité délivrant le moyen d'identification électronique, le demandeur devant être physiquement présent ;

    - Le document d'identité dispose de caractéristiques de sécurité exploitables à partir d'une photocopie ou d'une image numérisée ;

- La photocopie ou l'image numérisée est suffisamment fidèle et permet de réaliser l'ensemble des contrôles ultérieurs nécessaires. En particulier, elle doit être en couleur et présenter une résolution d'au moins 400 DPI ;

- Le même membre du personnel a été en capacité de réaliser un premier contrôle sur le document d'identité présenté physiquement, et en particulier a pu vérifier que le document d'identité n'a pas fait l'objet d'une falsification ou contrefaçon évidente.

- 2) Le document d'identité comporte des informations lisibles par une machine, intégrant l'ensemble des informations nécessaires à la délivrance du moyen d'identification électronique, et dont l'authenticité peut être prouvée via le recours à des moyens automatisés effectuant des vérifications cryptographiques. *Par exemple, un code barre 2D comportant des informations signées peut être un moyen de répondre à cette exigence. La bande « MRZ » ne permet pas d'y répondre.*

Cas de la vérification d'authenticité d'un document d'identité présenté lors d'un face à face à distance

La vérification d'authenticité d'un document d'identité présenté lors d'un face à face à distance, lorsque le document d'identité n'est présenté physiquement à aucune étape du processus de vérification *(par exemple lorsque le document est présenté par le biais d'un système de visio-conférence)* est considérée comme une méthode suffisante si les exigences du référentiel [PVID], pour le niveau de garantie substantiel, sont respectées.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

ou

3. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.2 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que ladite garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 du Parlement européen et du Conseil ou par un organisme équivalent ;

La confirmation de la garantie équivalente implique que les procédures précédemment utilisées conduisent à des résultats conformes aux exigences s'appliquant à chaque niveau de garantie.

La garantie équivalente est appréciée par l'organisme en charge de l'audit visé au II.2.4.7, et confirmée par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

ou

4. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel et tenant

compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé ou substantiel doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent.

Lorsque le demandeur dispose déjà d'un moyen d'identification électronique respectant les exigences applicables au niveau de garantie substantiel ou élevé, le fournisseur de moyen d'identification électronique n'est pas tenu de procéder à la vérification de son identité selon les modalités prévues dans le présent chapitre, sous réserve des deux conditions suivantes :

- Le demandeur doit procéder à une identification électronique avec le moyen d'identification électronique dont il dispose, en respectant les conditions d'usage et réserves éventuelles de ce moyen d'identification électronique ;

- Le recours à ce processus de délivrance simplifié est précédé par une analyse des risques de modification des données à caractère personnel relatives à l'identification du demandeur par le fournisseur de moyen d'identification électronique.

Le fournisseur de moyen d'identification électronique ne peut recourir à ce processus de délivrance simplifié si le moyen d'identification électronique présenté a lui-même déjà été délivré selon ce processus simplifié.

Le respect de ces exigences est apprécié par l'organisme en charge de l'audit visé au II.2.4.7, et confirmé par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

Les exigences du point 1 ou 2 ci-dessous doivent être respectées :

1. Niveau substantiel, plus l'une des options énumérées aux points a) à c) ci-dessous :

a. lorsqu'il a été vérifié que la personne est en possession d'un élément d'identification biométrique ou photographique reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et que cet élément correspond à l'identité alléguée, l'élément fait l'objet d'une vérification visant à déterminer sa validité selon une source faisant autorité ;

et

le demandeur est identifié comme ayant l'identité alléguée par comparaison d'une ou de plusieurs caractéristiques physiques de la personne auprès d'une source faisant autorité ;

La comparaison d'une ou plusieurs caractéristiques physiques doit être réalisée avec un niveau de fiabilité suffisant pour garantir que le demandeur est identifié comme ayant l'identité alléguée.

La fiabilité des procédures de vérification se traduit notamment par un faible taux de fausses concordances. Les facteurs permettant d'aboutir à un faible taux de fausses concordances incluent notamment la qualité des données de comparaison ainsi que la performance des algorithmes mis en œuvre, ou le niveau de formation des personnels impliqués.

Si le rapprochement automatisé est utilisé, la meilleure pratique disponible doit être prise en compte. *Par exemple, si le critère de comparaison est la photographie du demandeur, celle-ci doit être obtenue directement d'une source faisant autorité, et le mécanisme de reconnaissance faciale doit être éprouvé et résister aux attaques connues.*

Cas de la vérification d'authenticité d'un document d'identité présenté lors d'un face à face physique

Lorsque le document d'identité est vérifié lors d'une présentation physique, l'ensemble des caractéristiques de sécurité décrite dans le registre PRADO, selon le document d'identité concerné, doivent être vérifiées.

Le recours à du matériel spécifique peut être nécessaire (*lampe à ultra-violets, par exemple*).

Le personnel inspectant des documents physiques doit :

- avoir reçu une formation appropriée et disposer d'une bonne connaissance pratique de la conception des documents et de leurs caractéristiques de sécurité ;
- être capable d'identifier les documents falsifiés et contrefaits en les examinant ;
- être en mesure de faire bon usage des équipements de référence (*lampes UV par exemple*).

Cas de la vérification d'authenticité d'un document d'identité sur la base d'une photocopie ou d'une image numérisée

Lorsque la vérification d'authenticité du document d'identité s'appuie sur une photocopie ou une imagé numérisée, les exigences du niveau substantiel s'appliquent. En complément, la photocopie ou l'image numérisée doit présenter une résolution d'au moins 600 DPI, et le processus de vérification doit permettre d'inspecter l'ensemble des caractéristiques de sécurité du document.

Cas de la vérification d'authenticité d'un document d'identité présenté lors d'un face à face à distance

La vérification d'authenticité d'un document d'identité présenté lors d'un face à face à distance, lorsque le document d'identité n'est présenté physiquement à aucune étape du processus de vérification *(par exemple lorsque le document est présenté par le biais d'un système de visio-conférence)* est considérée comme une méthode suffisante si les exigences du référentiel [PVID], pour le niveau de garantie élevé, sont respectées.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

ou

b. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.2 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent

et

des mesures sont prises pour prouver que les résultats des procédures antérieures demeurent valides ;

Les données d'identité vérifiées précédemment peuvent être obsolètes, *par exemple en cas de changement de nom ou changement d'adresse*. Cette exigence vise à garantir que la validité des données d'identification soit vérifiée, et que ces données soient mises à jour si nécessaire.

La garantie équivalente est appréciée par l'organisme en charge de l'audit visé au II.2.4.7, et confirmée par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

c. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent

et

des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique notifié demeurent valides ;

Lorsque le demandeur dispose déjà d'un moyen d'identification électronique respectant les exigences applicables au niveau de garantie élevé, le fournisseur de moyen d'identification électronique n'est pas tenu de procéder à la vérification de son identité selon les modalités prévues dans le présent chapitre, sous réserve des deux conditions suivantes :

- Le demandeur doit procéder à une identification électronique avec le moyen d'identification électronique dont il dispose, en respectant les conditions d'usage et réserves éventuelles de ce moyen d'identification électronique ;

- Le recours à ce processus de délivrance simplifié est précédé par une analyse des risques de modification des données à caractère personnel relatives à l'identification du demandeur par le fournisseur de moyen d'identification électronique.

Le fournisseur de moyen d'identification électronique ne peut recourir à ce processus de délivrance simplifié si le moyen d'identification électronique présenté a lui-même déjà été délivré selon ce processus simplifié.

Le respect de ces exigences est attesté par l'Agence nationale de la sécurité des systèmes d'information.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

ou

2. lorsque le demandeur ne présente pas d'élément d'identification biométrique ou photographique reconnu, les mêmes procédures que celles utilisées au niveau national dans l'État membre de l'entité responsable de l'inscription afin d'obtenir ledit élément d'identification biométrique ou photographique reconnu sont appliquées.

Les procédures mises en œuvre pour la délivrance des cartes nationales d'identité, titres de séjour et passeports, peuvent être utilisées pour délivrer des moyens d'identification électronique.

II.2.1.3. Preuve et vérification d'identité (personne morale)

La vérification de l'identité d'une personne morale implique la vérification de l'identité de la personne physique représentant la personne morale et de son lien avec cette personne morale, dans les conditions prévues respectivement par les chapitres II.2.1.2 et II.2.1.4.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique.

L'identité alléguée d'une personne morale est établie sur la base de l'élément d'identification qui inclut :

- le nom de la personne morale (par exemple la raison sociale pour une entreprise) ; et
- son domicile ; et
- son numéro d'immatriculation (*par exemple le numéro SIREN pour les entreprises établies en France ou le numéro RNA pour certaines associations établies en France*).

Exemples de modalité de vérification de l'identité :

- *d'une entreprise établie en France : La vérification de l'identité d'une entreprise peut s'effectuer par la vérification d'un extrait « K-bis » de moins de trois mois ;*
- *d'une association établie en France : La vérification de l'identité d'une association peut s'effectuer par la vérification du récépissé de déclaration en préfecture de création ou de dernière modification éventuelle comportant le RNA ;*
- *d'une administration de l'État : La présentation de l'acte extrait du Journal officiel de la République française portant création et définissant les missions de cette administration.*

Pour les personnes morales établies dans d'autres pays que la France, les attachés commerciaux des consulats et des ambassades peuvent indiquer les éléments d'identification à considérer. *Par exemple, le numéro de TVA intracommunautaire pour une entreprise redevable de la TVA dans l'Union européenne (UE).*

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

2. L'élément d'identification semble être valide et on peut présumer qu'il est authentique ou qu'il existe selon une source faisant autorité, l'inscription d'une personne morale auprès de la source faisant autorité étant une démarche volontaire et régie par un accord entre la personne morale et la source faisant autorité.

Le terme « authentique » fait référence à l'authenticité de l'élément d'identification au moment de la délivrance. On peut présumer qu'il demeure authentique s'il n'a pas été falsifié ou manipulé. *Par exemple, le numéro d'immatriculation RNA doit avoir été délivré par la Préfecture*.

Le terme « validité » fait référence à l'exactitude de l'élément d'identification au moment de la présentation par le demandeur. *Cela peut concerner, par exemple, l'exactitude des informations contenues dans l'élément d'identification et son état de révocation/suspension.*

La vérification de l'élément d'identification doit permettre d'établir que cet élément n'a pas fait l'objet d'une falsification évidente détectable par des personnels non formés, et que les données d'identité nécessaires à l'inscription sont lisibles et cohérentes avec les données transmises dans la demande.

Exemple de vérification de l'authenticité des éléments d'identification d'une entreprise établie en France : lecture des informations présentes sur le K-bis transmis par le demandeur et recoupement avec les informations disponibles par ailleurs comme l'avis de situation au répertoire SIRENE.

Exemple de vérification de l'authenticité des éléments d'identification d'une entreprise établie hors de France : lecture des informations présentes sur un document présentant des garanties équivalente au K-bis et recoupement avec le site VIES de la Commission européenne.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

3. La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir en qualité de personne morale.

Il n'existe pas en France de source faisant autorité recensant les situations qui empêcheraient une personne morale d'agir en qualité de personne morale.

Pour les personnes morales établies dans d'autres pays que la France, les attachés commerciaux des consulats et des ambassades peuvent indiquer les sources faisant autorité à considérer.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

Niveau faible, plus l'une des options énumérées aux points 1 à 3 ci-après :

1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique, y compris le nom de la personne morale, sa forme juridique et (le cas échéant) son numéro d'immatriculation

Prescriptions identiques à celles fixées pour le niveau faible, point 1.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

et

l'élément d'identification est soumis à une vérification visant à déterminer s'il est authentique, ou si son existence est connue d'une source faisant autorité, l'inscription de la personne morale auprès de la source faisant autorité étant requise pour que la personne morale puisse exercer ses activités dans son secteur

La vérification de l'authenticité d'un élément d'identification d'une personne morale établie en France implique obligatoirement un recoupement de l'information communiquée par le demandeur par rapport aux sources faisant autorité reconnues par la France.

Par exemple pour les entreprises établies en France : la vérification, via le numéro SIREN figurant sur l'élément d'identification communiqué, de l'inscription au répertoire SIRENE est obligatoire. Pour les associations, la vérification de la publication au Journal officiel de la République française de la création de l'association est obligatoire.

Pour les personnes morales établies hors de France, une vérification d'authenticité de l'élément d'identification apportant une garantie équivalente doit être mise en œuvre. *Par exemple, pour une entreprise redevable de la TVA dans l'Union européenne (UE), le recoupement avec le site VIES de la Commission européenne est obligatoire.*

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

et

des mesures ont été prises pour minimiser le risque que l'identité de la personne morale ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration des documents ;

Exemple : pour une entreprise on procédera à i) vérification du K-bis daté de moins de trois mois, ii) à un recoupement avec les informations disponibles au répertoire SIRENE et sur VIES, et iii) à une vérification du pouvoir de la personne physique accomplissant les démarches (soit qu'elle soit mentionnée directement sur le K-bis en tant que mandataire social, soit qu'elle dispose d'une délégation de signature pour accomplir les démarches).

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

2. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.3 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent ;

La garantie équivalente est appréciée par l'organisme en charge de l'audit visé au II.2.4.7, et confirmée par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

ou

3. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé ou substantiel doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent.

Lorsque le demandeur dispose déjà d'un moyen d'identification électronique respectant les exigences applicables au niveau de garantie substantiel ou élevé, le fournisseur de moyen d'identification électronique n'est pas tenu de procéder à la vérification de son identité selon les modalités prévues dans le présent chapitre, sous réserve des deux conditions suivantes :

- Le demandeur doit procéder à une identification électronique avec le moyen d'identification électronique dont il dispose, en respectant les conditions d'usage et réserves éventuelles de ce moyen d'identification électronique ;

- Le recours à ce processus de délivrance simplifié est précédé par une analyse des risques de modification des données à caractère personnel relatives à l'identification du demandeur par le fournisseur de moyen d'identification électronique.

Le fournisseur de moyen d'identification électronique ne peut recourir à ce processus de délivrance simplifié si le moyen d'identification électronique présenté a lui-même déjà été délivré selon ce processus simplifié.

Le respect de ces exigences est apprécié par l'organisme en charge de l'audit visé au II.2.4.7, et confirmé par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

Niveau substantiel, plus l'une des options énumérées aux points 1 à 3 ci-après:

1. l'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique, y compris le nom de la personne morale, sa forme juridique et au moins un identifiant unique représentant la personne morale utilisé dans un contexte national

Prescriptions identiques à celles fixée pour le niveau faible, point 1.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

et

l'élément d'identification est soumis à une vérification visant à déterminer s'il est valide selon une source faisant autorité ;

Les vérifications et recoupements requis au niveau substantiel sont également requis au niveau élevé.

De plus ils doivent être assortis, pour les entreprises, d'une vérification des actes publiés au greffe (permettant notamment de voir si des actes ont eu lieu postérieurement à la date du K-bis communiqué). *Ces informations peuvent par exemple être obtenues auprès du registre du commerce et des sociétés du greffe du tribunal de commerce auprès duquel l'entreprise est enregistrée.*

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

ou

2. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.3 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent

et

des mesures sont prises pour prouver que les résultats de cette procédure antérieure demeurent valides ;

La confirmation de la garantie équivalente implique que les procédures précédemment utilisées conduisent à des résultats conformes aux exigences s'appliquant à chaque niveau de garantie.

La garantie équivalente est appréciée par l'organisme en charge de l'audit visé au II.2.4.7, et confirmée par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel. Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

ou

3. lorsque les moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent

et

des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique notifié demeurent valides.

Lorsque le demandeur dispose déjà d'un moyen d'identification électronique respectant les exigences applicables au niveau de garantie élevé, le fournisseur de moyen d'identification

électronique n'est pas tenu de procéder à la vérification de son identité selon les modalités prévues dans le présent chapitre, sous réserve des deux conditions suivantes :

- Le demandeur doit procéder à une identification électronique avec le moyen d'identification électronique dont il dispose, en respectant les conditions d'usage et réserves éventuelles de ce moyen d'identification électronique ;

- Le recours à ce processus de délivrance simplifié est précédé par une analyse des risques de modification des données à caractère personnel relatives à l'identification du demandeur par le fournisseur de moyen d'identification électronique.

Le fournisseur de moyen d'identification électronique ne peut recourir à ce processus de délivrance simplifié si le moyen d'identification électronique présenté a lui-même déjà été délivré selon ce processus simplifié.

Le respect de ces exigences est apprécié par l'organisme en charge de l'audit visé au II.2.4.7, et confirmé par l'ANSSI lors de la certification de conformité du moyen d'identification électronique au présent référentiel.

II.2.1.4. Lien établi entre les moyens d'identification électronique de personnes physiques et morales

Le cas échéant, pour établir un lien entre le moyen d'identification électronique d'une personne physique et le moyen d'identification électronique d'une personne morale (« lien établi »), les conditions suivantes s'appliquent :

1) Il doit être possible de suspendre et/ou de révoquer le lien établi. Le cycle de vie d'un lien établi (par exemple activation, suspension, renouvellement, révocation) doit être géré selon des procédures reconnues à l'échelle nationale.

2) La personne physique dont le moyen d'identification électronique est lié au moyen d'identification électronique de la personne morale peut déléguer l'établissement du lien à une autre personne physique sur la base de procédures reconnues à l'échelle nationale. Toutefois, la personne physique délégante reste responsable.

3) L'établissement du lien s'effectue comme suit :

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau faible ou supérieur.

Voir les exigences applicables à la vérification d'identité des personnes physiques au chapitre II.2.1.2, pour le niveau faible, substantiel ou élevé.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

2. Le lien a été établi sur la base de procédures reconnues à l'échelle nationale.

La liste suivante fournit des exemples de procédures reconnues à l'échelle nationale :

- *Pour les entreprises et les groupements d'intérêt économique, les mandataires sociaux sont identifiés sur le K-bis, daté de moins de trois mois, et peuvent également être identifiés au moyen du Registre national du Commerce et des Sociétés ;*

- *Pour les associations, les personnes physiques habilitées à agir au nom de l'association sont indiquées dans les statuts ; il appartient donc au demandeur de fournir la copie des statuts de l'association déclarée lors de la création ou lors de la dernière modification éventuelle assortie du récépissé de création ou de modification délivré par la préfecture ;*

- *Pour l'État, les personnes physiques habilitées à agir au nom de l'administration sont désignées au Journal officiel de la République française ou au bulletin officiel. Le demandeur doit fournir une copie de l'acte publié.*

Si la personne physique concernée par la demande n'est pas identifiée par le biais de l'une des procédures reconnues à l'échelle nationale, elle doit présenter un pouvoir signé l'autorisant à demander et disposer d'un moyen d'identification électronique au nom de la personne morale par une personne physique ayant droit, qui doit elle-même avoir été identifiée selon l'une de ces procédures.

Ce pouvoir doit être accompagné d'une copie du document d'identité de la personne physique habilitée, datée et signée par celle-ci. La liste des documents d'identité admis est définie au chapitre II.1 du présent document. Le document d'identité doit être en cours de validité et la copie doit être datée de moins de trois mois.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

3. La personne physique n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir au nom de la personne morale.

Les vérifications prévues au point 2 ci-dessus permettent de couvrir cette exigence.

Pour les personnes physiques disposant d'un pouvoir les autorisant à demander et disposer d'un moyen d'identification électronique au nom de la personne morale, on peut présumer que le fait qu'elles disposent de ce pouvoir implique qu'elles peuvent agir au nom de la personne morale.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

Point 3 du niveau faible, plus :

1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau substantiel ou élevé.

Prescriptions identiques aux exigences applicables à la vérification d'identité des personnes physiques au chapitre II.2.1.2, pour le niveau substantiel ou élevé.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

2. Le lien a été établi sur la base de procédures reconnues à l'échelle nationale, qui ont abouti à l'enregistrement du lien établi auprès d'une source faisant autorité.

Prescriptions identiques à celles fixées pour le niveau faible, point 2.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

3. Le lien établi a été vérifié sur la base d'informations provenant d'une source faisant autorité.

Prescriptions identiques aux exigences applicables à la vérification d'identité des personnes morales au chapitre II.2.1.3, pour le niveau substantiel ou élevé.

Les sources faisant autorité pour l'identité de la personne morale peuvent permettre d'attester du lien avec la personne physique.

Si la personne physique concernée par la demande n'est pas identifiée par la source faisant autorité, elle doit présenter un pouvoir signé l'autorisant à demander et disposer d'un moyen d'identification électronique au nom de la personne morale par une personne physique ayant droit, qui doit elle-même avoir été identifiée par cette source faisant autorité.

Ce pouvoir doit être accompagné d'une copie du document d'identité de la personne physique habilitée, datée et signée par celle-ci. La liste des documents d'identité admis est définie au chapitre II.1 du présent document. Le document d'identité doit être en cours de validité et la copie doit être datée de moins de trois mois.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

Point 3 du niveau faible et point 2 du niveau substantiel, plus :

1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau élevé.

Prescriptions identiques aux exigences applicables à la vérification d'identité des personnes physiques au chapitre II.2.1.2, pour le niveau élevé.

Si la personne physique concernée par la demande n'est pas identifiée par la source faisant autorité, elle doit présenter un pouvoir signé l'autorisant à demander et disposer d'un moyen d'identification électronique au nom de la personne morale par une personne physique ayant droit, qui doit elle-même avoir été identifiée par cette source faisant autorité.

Ce pouvoir doit être accompagné d'une copie du document d'identité de la personne physique habilitée, datée et signée par celle-ci. La liste des documents d'identité admis est définie au chapitre II.1 du présent document. Le document d'identité doit être en cours de validité et la copie doit être datée de moins de trois mois.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

2. Le lien a été vérifié sur la base d'un identifiant unique représentant la personne morale et utilisé dans le contexte national ; et sur la base d'informations représentant de façon unique la personne physique et provenant d'une source faisant autorité.

Prescriptions identiques aux exigences applicables à la vérification d'identité des personnes morales au chapitre II.2.1.3, pour le niveau élevé.

Les sources faisant autorité pour l'identité de la personne morale permettent également d'attester du lien avec la personne physique.

II.2.2. Gestion des moyens d'identification électronique

Il faut considérer dans cette section que les utilisateurs peuvent mettre en œuvre le moyen d'identification électronique depuis un environnement qui n'est pas de confiance.

II.2.2.1. Caractéristiques et conception des moyens d'identification électronique

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

1. Le moyen d'identification électronique utilise au moins un facteur d'authentification.

2. Le moyen d'identification électronique est conçu pour que l'émetteur prenne des mesures raisonnables afin de vérifier qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.

L'émetteur est le fournisseur du moyen d'identification électronique.

Par exemple, l'émetteur d'un moyen d'identification électronique basé sur un mot de passe peut mettre en œuvre les mesures suivantes :

- *Stockage du mot de passe sous une forme transformée par une fonction de hachage non réversible et itérative en faisant intervenir un sel aléatoire ;*

- *Détermination d'un nombre maximum de tentatives de saisie du mot de passe.*

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

1. Le moyen d'identification électronique utilise au moins deux facteurs d'authentification de différentes catégories.

L'utilisation complémentaire de plusieurs facteurs d'authentification de différentes catégories permet d'accroître le niveau de sécurité global du moyen d'identification électronique, dans la mesure où les différentes catégories de facteurs d'authentification ne sont pas sensibles aux mêmes menaces. *Par exemple, les mots de passe peuvent être observés ou enregistrés au moment où ils sont saisis, les facteurs d'authentification basés sur la possession peuvent être volés ou perdus, les systèmes basés sur des facteurs d'authentification inhérents peuvent être vulnérables à des éléments spécialement forgés par les attaquants (photographies, vidéos, empreintes digitales en latex, etc.).*

Une pratique courante consiste à associer un dispositif cryptographique matériel basé sur la possession à la connaissance d'une information secrète qui sera nécessaire pour le déverrouiller. *Un exemple pourrait être l'utilisation d'un mot de passe couplé à un élément matériel respectant*

le standard FIDO U2F. Ainsi, même en cas de perte ou de vol du dispositif, celui-ci ne pourra pas être utilisé à des fins d'authentification sans le mot de passe correspondant.

Afin de lever toute ambiguïté, il est précisé que les différents facteurs doivent être liés au même moyen d'identification électronique.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

2. Le moyen d'identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.

L'établissement d'un lien entre le moyen d'identification électronique et son utilisateur constitue un prérequis à son utilisation à des fins d'authentification.

Les moyens de cryptologie constitutifs du moyen d'identification électronique doivent au minimum faire l'objet d'une **qualification au niveau élémentaire du [RGS]** reposant sur une Certification de Sécurité de Premier Niveau (CSPN), sur la base d'une cible de sécurité validée par l'ANSSI.

Cette qualification permet de présumer que le moyen d'identification électronique, utilisé conformément aux conditions d'utilisation définies dans l'attestation de qualification des moyens de cryptologie qui le constituent, est utilisé uniquement sous le contrôle de la personne physique à qui il appartient.

Les secrets cryptographiques employés dans le cadre de l'identification d'un utilisateur auprès d'un service numérique, et dont la divulgation permettrait l'usurpation ou l'altération de l'identité de l'utilisateur, **sont utilisés pour une durée maximale de cinq ans**.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

Niveau substantiel, plus :

1. Le moyen d'identification électronique protège contre les doubles emplois et les manipulations ainsi que contre les attaquants à potentiel d'attaque élevé.

La protection contre les duplications et les altérations concerne le moyen d'identification électronique dans sa globalité et non chacun des facteurs d'authentification pris individuellement.

L'utilisation de plusieurs facteurs d'authentification vise à réduire le risque d'usurpation d'identité, dans la mesure où les différentes catégories de facteurs d'authentification ne sont pas sensibles aux mêmes menaces.

Exemples de protection contre les altérations et les doubles emplois spécifiques aux différents types de facteurs :

- *facteurs d'authentification basés sur la possession : utilisation d'un dispositif cryptographique matériel dont la résistance aux manipulations permet d'empêcher l'extraction de la clé hors du dispositif ou sa manipulation dans le dispositif par le biais de moyens physiques ou électroniques ;*

- *facteurs d'authentification inhérents : reconnaissance du vivant, environnement de confiance, faible taux de fausses concordances.*

Les moyens de cryptologie constitutifs du moyen d'identification électronique, utilisés sous le contrôle du fournisseur de moyen de d'identification électronique pour la génération et la conservation des secrets cryptographiques (*par exemple, les HSM*) employés dans le cadre de l'identification d'un utilisateur auprès d'un service numérique doivent faire l'objet d'une **qualification au niveau renforcé du [RGS]** reposant sur une certification selon les Critères Communs au niveau d'assurance EAL4 ou supérieur, augmenté des paquets d'assurance prévus par la qualification, sur la base d'une cible de sécurité validée par l'ANSSI.

De plus, les moyens de cryptologie constitutifs du moyen d'identification électronique utilisés sous le contrôle de l'utilisateur, hors de l'environnement maîtrisé par le fournisseur de moyen d'identification électronique, et dont l'utilisation frauduleuse permet, directement, l'usurpation ou l'altération de l'identité de l'utilisateur (*par exemple, une carte à puce*) doivent faire l'objet d'une **qualification au niveau renforcé du [RGS]** reposant sur une certification selon les Critères Communs au niveau d'assurance EAL4 ou supérieur, augmenté des paquets d'assurance prévus par la qualification, sur la base d'une cible de sécurité validée par l'ANSSI.

Enfin, les moyens de cryptologie constitutifs du moyen d'identification électronique utilisés sous le contrôle de l'utilisateur, hors de l'environnement maîtrisé par le fournisseur de moyen d'identification électronique, et dont l'utilisation frauduleuse permet de faciliter l'usurpation ou l'altération de l'identité de l'utilisateur sans la permettre directement (*par exemple, une application mobile*) doivent au minimum faire l'objet d'une **qualification au niveau élémentaire du [RGS]** reposant sur une Certification de Sécurité de Premier Niveau (CSPN), sur la base d'une cible de sécurité validée par l'ANSSI.

Ces qualifications permettent de présumer que le moyen d'identification électronique, utilisé conformément aux conditions d'utilisation définies dans les différentes attestations de qualification des moyens de cryptologie qui le constituent, est sous le contrôle exclusif de la personne physique à qui il appartient, qu'il protège contre les doubles emplois et les manipulations non autorisées, et qu'il résiste aux attaquants à potentiel d'attaque élevé.

Les secrets cryptographiques manipulés par un moyen d'identification électronique de niveau élevé, dont la divulgation permettrait l'usurpation ou l'altération de l'identité de l'utilisateur, **sont utilisés pour une durée maximale de cinq ans**.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

2. Le moyen d'identification électronique est conçu de sorte que la personne à laquelle il appartient puisse le protéger de façon fiable contre toute utilisation non autorisée.

L'expression « protéger de façon fiable » fait référence aux efforts mis en œuvre afin d'empêcher que le moyen d'identification électronique soit utilisé sans que l'utilisateur en ait connaissance et sans qu'il y ait activement consenti. *Par exemple, une clé privée dans un dispositif cryptographique ne doit pas être utilisable sans le consentement actif de l'utilisateur. Ce consentement peut être manifesté par la saisie d'un code secret associé à ce dispositif cryptographique et connu uniquement de cet utilisateur.*

II.2.2.2. <u>Délivrance, mise à disposition et activation</u>

<u>Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE</u>

Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il ne sera reçu que par le destinataire prévu.

Pour le niveau faible, on peut présumer que seul le destinataire a accès à son compte de messagerie courriel ou son téléphone qui sont des moyens de communication personnels. Le destinataire doit être le futur utilisateur du moyen d'identification électronique.

Ainsi, par exemple dans le cadre de l'utilisation d'un facteur de connaissance de type mot de passe, celui-ci peut être activé par un lien contenant un code d'activation aléatoire envoyé à l'adresse courriel du destinataire ou par un code aléatoire d'activation envoyé par SMS au numéro de mobile du destinataire fourni lors de la phase d'enregistrement.

<u>Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL</u>

Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il sera exclusivement remis en la possession de la personne à laquelle il appartient.

Le mécanisme de mise à disposition doit reposer sur un processus d'activation pour lequel on peut raisonnablement présumer que seul l'utilisateur dispose des informations nécessaires à l'activation du moyen (*par exemple, un code PIN de transport délivré séparément du moyen d'identification électronique).*

Au niveau de garantie substantiel, plusieurs facteurs d'authentification doivent être utilisés. Plusieurs combinaisons de délivrance, de mise à disposition et d'activation remplissant les exigences du niveau substantiel sont possibles.

Les mécanismes envisageables pour la mise à disposition d'un facteur basé sur la possession, lorsque celui-ci est un dispositif matériel, sont les suivants :

- la remise en personne ; ou
- l'envoi en courrier recommandé.

Par exemple, le processus de mise à disposition d'un tel dispositif pourrait être constitué :

- *de la remise en face à face ou l'envoi par courrier recommandé d'un dispositif matériel cryptographique (FIDO U2F, ou générateur d'OTP) ; et*
- *de l'envoi par courrier simple, courriel ou SMS d'un lien ou d'un code d'activation permettant de définir le mot de passe du dispositif.*

Dans le cas où un facteur basé sur la possession n'est pas matériel (*par exemple, une application installée sur un téléphone mobile),* il est nécessaire d'assurer que celui-ci soit bien délivré sur un dispositif appartenant à l'utilisateur à l'aide d'un processus d'authentification et d'appairage.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

Le processus d'activation vérifie que le moyen d'identification électronique a été remis exclusivement en la possession de la personne à laquelle il appartient.

Cette vérification requiert l'exécution d'un processus d'activation. La seule mise à disposition sécurisée n'est pas suffisante. En principe, un processus d'activation nécessite une interaction de l'utilisateur.

L'objectif d'un processus d'activation – au-delà de garantir que le moyen est mis à la disposition de l'utilisateur auquel il appartient– est que l'utilisateur mette en œuvre une mesure explicite afin de prendre possession du moyen. Ce n'est qu'après cela que le moyen peut être utilisé à des fins d'identification électronique.

Au niveau de garantie élevé, le processus d'activation doit garantir que seul l'utilisateur est en mesure d'activer le moyen d'identification électronique et le processus d'activation doit être protégé contre la perte accidentelle du moyen d'identification électronique et les menaces internes au fournisseur de moyens d'identification électronique telles que la collusion.

S'ils sont assurés par des personnes physiques, l'enregistrement et l'émission d'un moyen d'identification électronique ne doivent jamais être effectués par une seule et même personne.

Lorsque des codes d'activation sont utilisés, le demandeur doit les mettre en œuvre dans un délai déterminé.

Par exemple, le processus d'activation peut consister en une remise en présence physique de l'utilisateur, après vérification de l'identité selon les exigences du règlement, d'un dispositif matériel cryptographique dont le code d'activation est choisi par l'utilisateur.

II.2.2.3. Suspension, révocation et réactivation

Dans le cas de la tutelle, le tuteur peut faire une demande de suspension, de révocation ou de réactivation pour le compte de la personne sous sa tutelle. Dans cette situation, le fournisseur de moyen d'identification électronique contrôle, en plus de l'identité de la personne sous tutelle, l'identité du tuteur ainsi que le dernier jugement de tutelle.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

1. Il est possible de suspendre et/ou de révoquer un moyen d'identification électronique de manière rapide et efficace.

Cette opération doit être accessible à l'utilisateur. *Par exemple, elle devrait pouvoir être effectuée par téléphone, via un site Internet, par le biais d'une adresse e-mail, etc.*

La fonction de gestion de suspension et de révocation doit être disponible 24h/24 et 7j/7.

Toute demande authentifiée de suspension ou de révocation d'un moyen d'identification électronique doit être traitée dans un délai inférieur à 24h. Ce délai s'entend entre la réception de la demande et la mise à disposition de l'information de suspension ou révocation auprès des tiers.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

2. Des mesures ont été prises pour prévenir toute suspension, révocation et/ou réactivation non autorisées.

À l'exception des personnes et entités identifiées dans les conditions générales d'utilisation, seul l'utilisateur du moyen d'identification électronique ou, dans le cas d'une personne morale, un représentant légal de cette personne morale peuvent demander une suspension ou une révocation.

Le fournisseur de moyen d'identification électronique peut également décider d'une révocation s'il a connaissance de l'une des causes de révocation suivantes :

- l'utilisateur n'a pas respecté ou ne respecte plus les conditions générales d'utilisation du moyen d'identification électronique ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- le moyen d'identification électronique ou les données d'activation associées sont suspectés de compromission, sont compromis, sont perdus ou volés ;
- l'utilisateur est décédé ;
- l'utilisateur a porté plainte pour usurpation d'identité.

L'utilisateur doit être informé, par le biais des conditions générales d'utilisation, des personnes et entités susceptibles d'effectuer une demande de suspension ou de révocation.

Si la demande de révocation est faite via un service téléphonique ou via un service en ligne, le demandeur de la révocation doit être formellement authentifié : le destinataire de la demande doit vérifier l'identité du demandeur de la révocation et son autorité par rapport au moyen d'identification électronique à révoquer (*par exemple, la vérification d'identité peut s'appuyer sur des réponses à des questions secrètes, et la vérification de l'autorité peut s'appuyer sur la liste des personnes et entités déclarées dans les conditions générales d'utilisation comme pouvant demander une révocation*).

Le demandeur doit être informé, par le biais des conditions générales d'utilisation, que ses informations personnelles d'identité pourront être utilisés comme éléments d'authentification lors de la demande de suspension ou de révocation, dans le cas où le fournisseur de moyen d'identification électronique s'appuie sur un tel mécanisme. En complément ou à la place de l'utilisation de ces informations personnelles, il pourra être convenu d'un jeu de questions/réponses ou d'un mécanisme équivalent.

Une demande de révocation peut également être faite par courrier ou par voie électronique. Elle doit alors être signée par le demandeur et le service de gestion des demandes de révocation doit s'assurer de l'identité du demandeur (*par exemple, vérification de la signature manuscrite par rapport à une signature préalablement enregistrée, ou de la signature électronique si l'envoi est fait par voie électronique*) et de son autorité par rapport au moyen d'identification électronique à révoquer.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

3. La réactivation ne pourra avoir lieu que si les exigences de garantie établies avant la suspension ou la révocation sont toujours respectées.

La réactivation d'un moyen d'identification électronique n'est possible que si les procédures utilisées pour la preuve et la vérification d'identité, et la délivrance initiale du moyen d'identification électronique, ou des procédures offrant un niveau d'assurance équivalent, sont mises en œuvre.

II.2.2.4. <u>Renouvellement et remplacement</u>

Dans le cas de la tutelle, le tuteur peut faire la demande de renouvellement ou de remplacement pour le compte de la personne sous tutelle. Dans cette situation, la vérification d'identité mentionnée dans cette section vise la personne sous tutelle.

<u>Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL</u>

En tenant compte des risques d'une modification des données d'identification personnelles, le renouvellement ou le remplacement doit satisfaire aux mêmes exigences de garantie que la preuve et la vérification d'identité initiales ou reposer sur un moyen d'identification électronique valide ayant un niveau de garantie identique ou supérieur.

Dans un délai de cinq ans à compter de la dernière vérification d'identité de l'utilisateur du moyen d'identification électronique, si ce moyen d'identification électronique n'a pas fait l'objet d'un renouvellement ou d'un remplacement, le fournisseur du moyen d'identification électronique doit procéder à une nouvelle vérification de l'identité visant à s'assurer que l'utilisateur est toujours la personne légitime à utiliser le moyen d'identification électronique présenté.

<u>Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ</u>

Niveau faible, plus :

Lorsque le renouvellement ou le remplacement est basé sur un moyen d'identification électronique valide, les données d'identité sont vérifiées auprès d'une source faisant autorité.

Les exigences en matière de preuve et de vérification de l'identité peuvent être remplies en s'appuyant sur un moyen d'identification électronique valide déjà existant, sous réserve que, pour la délivrance de ce premier moyen d'identification électronique, la preuve et la vérification d'identité aient été réalisées selon une autre méthode (*par exemple, ce premier moyen d'identification électronique a été délivré après une vérification d'identité lors d'un face-à-face physique*).

Il doit exister une preuve du respect de cette exigence pour le premier moyen d'identification électronique (*par exemple, la description du schéma d'identification électronique dans le cadre duquel est délivré ce moyen spécifie explicitement que la vérification d'identité ne peut être réalisée via l'utilisation d'un autre moyen d'identification électronique*).

En l'absence de norme identifiée permettant l'accréditation d'organismes d'évaluation de la conformité, la garantie équivalente est appréciée au cas par cas par l'ANSSI lors de l'évaluation de la conformité du moyen d'identification électronique au présent référentiel.

II.2.3. Authentification

La présente section met l'accent sur les menaces liées à l'utilisation du mécanisme d'authentification et répertorie les exigences applicables à chaque niveau de garantie. Dans la présente section, les contrôles sont censés être proportionnés aux risques au niveau donné.

II.2.3.1. Mécanisme d'authentification

Les mécanismes d'authentification utilisés lors de la phase d'authentification ne sont pas en mesure de contrer toutes les attaques ; ils ne résistent qu'aux attaquants dotés d'un certain potentiel d'attaque.

Lors de l'évaluation de la résistance, le mécanisme d'authentification doit être pris en compte dans sa globalité, y compris les risques découlant du processus de vérification de possession du moyen d'identification électronique.

Par exemple :

- *pour le niveau de garantie élevé, il ne suffit pas qu'une carte à puce protège une clé cryptographique contre les manipulations non autorisées ; en outre, le protocole cryptographique doit protéger le mécanisme de vérification de la possession de la clé contre les manipulations non autorisées et les attaques par rejeu ;*

- *pour les dispositifs utilisant des mots de passe à usage unique, lorsque le mot de passe à usage unique généré est transmis par le biais d'un canal sécurisé (par exemple, TLS), la force du facteur basé sur la possession est limitée non seulement par la force du dispositif, mais également par celle du canal sécurisé ;*

- *le mécanisme mis en œuvre pour établir la preuve de la possession d'un générateur de mots de passe temporaires à usage unique consiste à soumettre un mot de passe à usage unique généré au vérificateur. La force de ce mécanisme est limitée, entre autres, par la longueur du mot de passe à usage unique, l'échéance de la validité du mot de passe et la confidentialité de la transmission.*

Les mécanismes d'authentification reposant sur la cryptographie doivent être conformes aux règles définies dans le document [RGS_B1].

Des hypothèses raisonnables quant à l'environnement dans lequel est utilisé le moyen d'identification électronique doivent être prises en compte dans l'évaluation du risque.

À titre d'exemple, l'évaluation peut présumer que l'utilisateur fait usage d'un pare-feu et d'un antivirus personnels sur son ordinateur et que les logiciels sont à jour (en particulier le navigateur et le système d'exploitation).

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

1. La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité.

La diffusion de données d'identification personnelles consiste à transmettre à la partie utilisatrice l'ensemble minimal de données inscrites en annexe du règlement d'exécution [2015/1501].

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

2. Lorsque des données d'identification personnelle sont mémorisées dans le cadre du mécanisme d'authentification, ces informations sont sécurisées afin d'assurer leur protection contre toute perte ou compromission, y compris une analyse hors ligne.

Les données personnelles mémorisées doivent être soumises à des contrôles stricts en matière d'accès. Des mesures doivent être mises en œuvre afin de protéger les données d'identification personnelle, *par exemple, chiffrement et calcul d'empreinte conformément aux recommandations présentes dans le document [RGS_B1]*.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

3. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque de base renforcé puissent nuire aux mécanismes d'authentification.

Toutes les mesures de vérification du moyen d'identification électronique vis-à-vis des risques énumérés doivent être décrites de manière claire, mises en œuvre et testées.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

Niveau faible, plus :

1. La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique.

En pratique, cela signifie que le moyen d'identification électronique doit inclure un code à usage unique ou un défi-réponse afin de garantir qu'il est véritablement dynamique. Le code à usage unique ou le défi-réponse doit être généré et transporté de point à point de façon sécurisée de sorte qu'il ne puisse être manipulé.

Lorsque des nombres aléatoires sont utilisés dans un protocole défi-réponse, il convient de s'assurer de la « qualité » de ces nombres, *par exemple en se conformant aux bonnes pratiques relatives à l'utilisation de générateurs de nombres pseudo-aléatoires sécurisés par chiffrement conformément aux recommandations présentes dans le document [RGS_B1]*.

Note : pour les niveaux substantiel et élevé, l'usage du simple texto transmis non chiffré (« OTP SMS ») est à prohiber en raison du risque important d'interception malveillante.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

2. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles

que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.

La part du mécanisme d'authentification portée par le serveur, communiquant avec le moyen d'identification électronique, doit être mise en œuvre au moyen d'un moyen de cryptologie ayant au minimum été **qualifié par l'ANSSI au niveau élémentaire du [RGS]**, sur la base d'une Certification de Sécurité de Premier Niveau (CSPN), et utilisé conformément aux conditions d'utilisation définies dans son attestation de qualification.

En complément, il est recommandé que les autres moyens de cryptologie (*par exemple, des applications*) intervenant, le cas échéant, dans le processus d'authentification fassent l'objet d'une **qualification par l'ANSSI au niveau élémentaire du [RGS]**. Dans le cas contraire, il doit être démontré la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur ces moyens.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

Niveau substantiel, plus :

Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque élevé puissent nuire aux mécanismes d'authentification.

La part du mécanisme d'authentification portée par le serveur, communiquant avec le moyen d'identification électronique, doit être mise en œuvre au moyen d'un moyen de cryptologie ayant été **qualifié par l'ANSSI au niveau renforcé du [RGS]**, sur la base d'une certification selon les Critères Communs au niveau d'assurance EAL4 augmenté des paquets d'assurance prévus par la qualification, et utilisé conformément aux conditions d'utilisation définies dans son attestation de qualification.

En complément, il est recommandé que les autres moyens de cryptologie intervenant, le cas échéant, dans le processus d'authentification fassent l'objet d'une **qualification par l'ANSSI au niveau élémentaire du [RGS], ou supérieur en fonction des risques identifiés**. Dans le cas contraire, il doit être démontré la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur ces applications.

Cette qualification est obligatoire pour les moyens de cryptologie exécutés dans un environnement qui n'est pas de confiance. L'ANSSI détermine le niveau de qualification adéquat pour ces moyens.

II.2.4. Gestion et organisation

Tous les participants fournissant un service lié à l'identification électronique dans un contexte transfrontalier («fournisseurs») doivent disposer de pratiques de gestion de la sécurité de l'information documentées, de politiques, d'approches de la gestion des risques et d'autres contrôles reconnus afin de garantir aux organes de gouvernance appropriés responsables des schémas

d'identification électronique dans les différents États membres que des pratiques efficaces sont en place. Tous les éléments/exigences figurant au point 2.4 sont censés être proportionnés aux risques au niveau donné.

La dénomination « Tous les participants » inclut les parties prenantes dans le processus d'authentification transfrontalier, y compris le fournisseur d'identité mais exclut les administrations en charge de la gestion des sources faisant autorité.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], toutes les exigences des chapitres II.2.4.4 à II.2.4.6 étant couvertes par les contrôles appropriés mentionnés dans ladite norme.

II.2.4.1. Dispositions générales

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

1. Les fournisseurs fournissant un service opérationnel visé par le présent règlement sont une autorité publique ou une personne morale reconnue comme telle par le droit national d'un État membre, avec une organisation établie et pleinement opérationnelle à tous les égards pertinents pour la fourniture des services.

2. Les fournisseurs respectent toute exigence légale qui leur incombe dans le cadre du fonctionnement et de l'exécution du service, y compris les types d'informations pouvant être recherchés, la façon dont la preuve d'identité est établie, le type d'informations pouvant être conservées et leur durée de conservation.

3. Les fournisseurs sont en mesure de démontrer leur capacité à assumer la responsabilité d'éventuels dommages, ainsi que le fait qu'ils disposent de ressources financières suffisantes pour la poursuite de leurs activités et la fourniture des services.

Il peut être présumé qu'une administration de l'État dispose des ressources financières suffisantes pour assumer toute responsabilité au sens des points 2 et 3 du règlement d'exécution ci-dessus.

Un autre moyen permettant de démontrer que cette exigence est satisfaite peut par exemple être la souscription d'une assurance suffisante au regard des obligations.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

4. Les fournisseurs sont responsables de l'exécution de toute tâche sous-traitée à une autre entité, ainsi que du respect de la politique du schéma, comme s'ils s'étaient acquittés eux-mêmes de leur mission.

Cela implique notamment que toute entité sous-traitante doit pouvoir se soumettre à un audit de son organisation, dans les mêmes conditions que le fournisseur du moyen d'identification électronique, et que les résultats de cet audit doivent être portés à la connaissance de ce fournisseur.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

5. Les schémas d'identification électronique non constitués par le droit national doivent mettre en place un plan de cessation d'activités efficace. Ce plan comporte des mesures concernant l'organisation en cas d'arrêt de fourniture du service ou de la reprise de la fourniture par un autre fournisseur, la façon dont les autorités compétentes et les utilisateurs finaux sont informés, ainsi que des détails sur les modalités de protection, conservation et destruction des informations conformément à la politique du schéma.

Cela concerne à la fois l'arrêt de fourniture du service relatif au schéma d'identification électronique et la fermeture par des autorités externes. Ces plans doivent couvrir l'ensemble des circonstances prévisibles menant à l'arrêt de fourniture du service ou à la reprise de la fourniture par un autre fournisseur.

II.2.4.2. Avis publiés et information des utilisateurs

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

1. Il doit exister une définition de service publiée qui inclut toutes les modalités, conditions et frais applicables, y compris les éventuelles limitations de son utilisation. La définition de service doit inclure une politique de confidentialité.

Le fournisseur du moyen d'identification électronique publie cette définition de service dans ses conditions générales d'utilisation qui reprennent les informations suivantes :

- la mention du type de population à laquelle les moyens d'identification électronique peuvent être délivrés (*par exemple des professionnels, des agents de l'administration, des personnes résidant en France…)* ;
- les exigences en matière de protection des moyens d'identification électronique ;
- les conditions d'usages des moyens d'identification électronique et leurs limites ;
- les obligations et responsabilités des différentes parties ;
- les garanties et limites de garanties du fournisseur de moyen d'identification électronique ;
- la durée de conservation des dossiers d'enregistrement et des journaux d'évènements ;
- les procédures pour la résolution des réclamations et des litiges ;
- le système légal applicable ;
- le niveau de garantie du moyen d'identification électronique ;
- la politique de confidentialité ;
- tous les frais applicables à la demande, à l'utilisation ou au renouvellement du moyen d'identification électronique.

Ces conditions générales font notamment partie intégrante du dossier d'enregistrement et doivent être explicitement acceptées par le demandeur.

Le moyen utilisé pour la publication de ces informations est libre mais doit permettre de garantir l'intégrité, la lisibilité et la clarté des informations publiées.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

2. Il convient de mettre en place des procédures et politiques appropriées permettant de garantir que les utilisateurs du service sont informés de façon fiable et rapide de tout changement apporté à la définition de service et à toute modalité, condition et politique de confidentialité applicable relative au service spécifié.

Dans ce contexte, « informés » ne signifie pas nécessairement que les informations doivent systématiquement être adressées individuellement à tous les utilisateurs de moyen d'identification électronique. Cette information peut également se faire à travers la publication des éléments requis sur le site Internet du fournisseur, en fonction de la nature du changement. Il est toutefois recommandé qu'une alerte soit envoyée aux utilisateurs, les incitant à consulter ces nouvelles informations.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

3. Il y a lieu de mettre en place des procédures et politiques appropriées permettant d'apporter des réponses complètes et exactes aux demandes de renseignements.

En particulier, le fournisseur de moyen d'identification électronique met en place les politiques et procédures nécessaires pour permettre à l'utilisateur d'exercer ses droits prévus aux articles 15, 16, 17, 18, 20 et 21 du [RGPD], sous réserve de compatibilité avec les autres exigences applicables au titre du présent référentiel (*par exemple, l'utilisateur doit pouvoir exercer son droit de rectification ou de suppression sur les données le concernant. Cependant, l'exercice de ces droits ne doit pas affecter les données archivées pour des raisons de résolution des litiges).*

II.2.4.3. Gestion de la sécurité de l'information

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

Il existe un système de gestion de la sécurité de l'information efficace pour la gestion et le contrôle des risques de sécurité de l'information.

La gestion des risques liés à la sécurité de l'information est pertinente pour tous les aspects du schéma d'identification électronique. Afin d'être efficace, le système de gestion de la sécurité de l'information doit prendre en compte les risques afférant à tous les aspects du schéma. En particulier, le fournisseur de moyen d'identification électronique met en place les processus et procédures permettant la sécurisation du traitement de données biométriques, si un tel traitement existe, dans le respect de la réglementation en matière de protection des données à caractère personnel [RGPD] et [LIL].

En fonction de la structure organisationnelle du schéma d'identification électronique, il est recommandé de recourir à plusieurs systèmes de gestion de la sécurité de l'information pour les différents opérateurs des éléments du schéma.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL, ÉLEVÉ
Niveau faible, plus : Le système de gestion de la sécurité de l'information adhère à des normes ou principes éprouvés pour la gestion et le contrôle des risques de sécurité de l'information.

La norme [ISO_27001] représente une norme réputée et éprouvée en matière de gestion des risques de sécurité de l'information, et il est recommandé de la mettre en œuvre. À défaut, il est nécessaire de démontrer que le système de gestion de la sécurité de l'information adhère à des normes ou principes apportant un niveau de sécurité similaire.

II.2.4.4. Conservation d'informations

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ
1. Enregistrer et conserver les informations pertinentes à l'aide d'un système efficace de gestion des informations, en tenant compte de la législation applicable et des bonnes pratiques en matière de protection et de conservation des données.

Le système de gestion des informations doit journaliser les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;

- les changements apportés au personnel ;

- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs,...) ;

- la réception d'une demande de moyen d'identification électronique (initiale et renouvellement) ;

- la validation ou le rejet d'une demande de moyen d'identification électronique ;

- les évènements liés à la gestion des matériels cryptographiques sensibles et des clés qu'ils mettent en œuvre (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;

- le cas échéant, la génération des éléments secrets de l'utilisateur (bi-clé, codes d'activation,…) ou publics (certificats…) ;

- la transmission des moyens d'identification électronique aux utilisateurs et, selon les cas, les acceptations ou rejets explicites par les utilisateurs ;

- le cas échéant, la remise de son moyen d'identification électronique à l'utilisateur ;

- la publication et mise à jour des conditions générales d'utilisation ou autres documents publiés par l'entité responsable du schéma d'identification électronique ;

- la réception d'une demande de révocation ;

- la validation ou le rejet d'une demande de révocation ;

- si le moyen d'identification électronique met en œuvre des certificats, la génération et la publication des LCR (et éventuellement des deltaLCR) ou des requêtes / réponses OCSP.

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en intégrité et en disponibilité (contre la perte, l'altération et la destruction partielle ou totale, volontaire ou non).
Pour dater ces évènements, il est possible de recourir :

- soit à un service d'horodatage électronique tel que prévu par le règlement [eIDAS], interne ou externe ;

- soit à l'heure système et en assurant une synchronisation des horloges des systèmes entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne, cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système

devra toutefois pouvoir ordonner les évènements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

Selon la nature des informations traitées, il peut être nécessaire d'assurer la protection en confidentialité des journaux d'événements.

Les journaux d'événement doivent faire l'objet d'une analyse quotidienne, et un mécanisme de remontée d'alerte doit être mis en place. Tous les journaux d'événement doivent être corrélés de manière hebdomadaire.

En complément des journaux, le système de gestion des informations doit couvrir les éléments suivants :

- les politiques et procédures appliquées aux fins de délivrance, renouvellement et révocation des moyens d'identification électronique ;
- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres entités ;
- le cas échéant, les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- le cas échéant, les politiques de certification encadrant la délivrance des certificats électroniques ;
- les récépissés ou notifications (à titre informatif) ;
- L'ensemble des informations transmises par les utilisateurs pour justifier de leur identité et, le cas échéant, de celle de leur entité de rattachement, dans le cadre du processus de délivrance du moyen d'identification électronique.

Le système de gestion des informations doit être mis en œuvre conformément à la législation applicable en matière de protection des données à caractère personnel, notamment le [RGPD].

En particulier :

- Les données conservées à des fins d'archivage ne peuvent pas faire l'objet de traitement biométrique. La photographie du demandeur (incluant le cas échéant la photographie présente sur un document d'identité archivé) ne peut être conservée à des fins d'archivage que si le fournisseur de moyen d'identification électronique met en œuvre l'ensemble des mesures organisationnelles et techniques nécessaires pour protéger cette photographie contre les accès non autorisés (*par exemple en recourant au chiffrement de ces données*), et pour interdire tout accès à la photographie archivée en dehors du strict besoin d'enquête et de résolution des litiges. Les empreintes digitales ne doivent pas être conservées.

- La conservation des données dont la finalité est de faire l'objet d'un traitement biométrique ne doit pas excéder quatre-vingt-seize heures à compter du recueil desdites données.

- Le fournisseur doit préciser la ou les finalités de conservation des données à caractère personnel des utilisateurs.

- Il est recommandé que le fournisseur s'appuie sur le guide [CNIL_Guide_conservation] pour définir les durées et modalités de conservation.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.12 « Sécurité liée à l'exploitation » (en particulier A.12.4 « Journalisation et surveillance ») associés à ceux visés au point A.18 « Conformité ».

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

2. Conserver, autant qu'il est permis par la législation nationale ou par tout autre arrangement administratif national, et protéger les informations pendant aussi longtemps qu'elles sont nécessaires pour auditer et enquêter sur les atteintes à la sécurité, et à des fins de conservation, après quoi les informations doivent être détruites en toute sécurité.

Les informations, en particulier celles utilisées aux fins de la non-répudiation, doivent être conservées le temps jugé nécessaire au regard de l'objectif d'usage en particulier pour être utilisées à l'appui de tout litige ou procédure juridique, et pour une durée de cinq ans à compter de la dernière vérification d'identité de l'utilisateur du moyen d'identification électronique pour les moyens d'identification électronique visant le niveau de garantie substantiel ou élevé.

Le référentiel ne définit pas de durée de conservation pour les moyens d'identification électronique visant le niveau de garantie faible. Au regard du principe de responsabilisation, il importe au fournisseur de moyen d'identification électronique, en tant que responsable de traitement, de définir une durée de conservation. Cette durée de conservation est proportionnée à la finalité du traitement.

Ces informations doivent être détruites lorsqu'elles ne sont plus nécessaires.

La destruction concerne tous les supports, qu'ils soient électroniques ou physiques, sur lesquels ces informations sont conservées.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.18 « Conformité » (cf. A.18.1.3 « Protection des enregistrements »).

II.2.4.5. Installations et personnel

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

1. Il existe des procédures garantissant que le personnel et les sous-traitants sont suffisamment formés, qualifiés et expérimentés eu égard aux compétences nécessaires pour exécuter les tâches qui leur sont confiées.

Lorsqu'il est nécessaire que le personnel dispose de compétences spécifiques pour exécuter des tâches qui lui sont confiés, un programme de formation visant à garantir que le personnel est en mesure de démontrer et de conserver ces compétences doit être mis en place.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.7 « Sécurité des ressources humaines » (cf. en particulier A.7.2.2 « Sensibilisation, apprentissage et formation à la sécurité de l'information »).

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

2. Le personnel et les sous-traitants doivent être en nombre suffisant pour faire fonctionner et gérer de manière adéquate le service conformément à ses politiques et procédures.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.12 « Sécurité liée à l'exploitation » (cf. A.12.1.3 « Dimensionnement »), qui traite également de la capacité des ressources humaines.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

3. Les installations utilisées pour fournir le service sont surveillées en permanence et protégées contre les dommages causés par des événements environnementaux, l'accès non autorisé et d'autres facteurs susceptibles d'avoir une incidence sur la sécurité du service.

Les services présentant des exigences de sécurité critiques, par exemple la révocation, doivent résister aux pannes et aux interruptions de service. Les mesures mises en place doivent garantir au service un niveau de protection suffisant contre les pannes et les évènements naturels tels que les incendies, les inondations, les orages ou les tremblements de terre, qui affectent une installation unique.

Par exemple, la mise en place, dans le cadre d'un plan de continuité d'activité, d'un site secondaire situé à une distance suffisante du site principal, peut être nécessaire pour assurer la continuité ou la reprise d'activité en cas de sinistre.

Le cas échéant, les installations physiques doivent être sécurisées au moyen de serrures appropriées et de mécanismes de contrôle d'accès ainsi que par une surveillance physique (*par exemple, vidéosurveillance*). Ces moyens peuvent être fournis par l'exploitant de l'installation à titre de service.

Il doit exister un processus visant à détecter les accès non autorisés et à alerter le service d'identification en cas de survenue d'évènements non autorisés.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés aux points A.11 « Sécurité physique et environnementale » et A.9 « Contrôle d'accès ». Les

mécanismes de surveillance doivent également être considérés comme relevant des contrôles visés au point A.12 « Sécurité liée à l'exploitation ».

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE, SUBSTANTIEL, ÉLEVÉ

4. Les installations utilisées pour fournir le service garantissent que l'accès aux zones de conservation ou de traitement d'informations personnelles, cryptographiques ou autres informations sensibles est limité au personnel ou aux sous-traitants autorisés.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés aux points A.9 « Contrôle d'accès », dont l'objectif est notamment de limiter l'accès aux informations et aux installations de traitement des informations, et A.10 « Cryptographie ».

II.2.4.6. Contrôles techniques

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

1. Il existe des contrôles techniques proportionnés pour gérer les risques menaçant la sécurité des services, en protégeant la confidentialité, l'intégrité et la disponibilité de l'information traitée.

Il est obligatoire d'appliquer l'ensemble des règles de niveau « standard » définies dans le guide d'hygiène informatique [GH] publié par l'ANSSI. Il est recommandé d'appliquer les règles de niveau « renforcé ».

Il convient de distinguer l'évaluation relative aux exigences de protection en matière de confidentialité de celle relative aux exigences de protection en matière d'intégrité. Là où la protection de l'intégrité (ou authenticité) est essentiellement déterminée par le niveau de garantie visé, la confidentialité des données personnelles doit également prendre en compte la nature des données ainsi que les éventuelles exigences légales en matière de protection des données.

La confidentialité des données personnelles doit être protégée, des contrôles doivent avoir été mis en place sur la base d'une évaluation utilisant une approche basée sur le risque conforme au système de gestion de la sécurité de l'information.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés aux points A.10 « Cryptographie », A.12 « Sécurité liée à l'exploitation », (concernant la disponibilité) A.17 « Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité » et A.18.1.5 « Règlementation relative aux mesures cryptographiques ».

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

2. Les canaux de communication électronique utilisés pour échanger des informations personnelles ou sensibles sont protégés contre les écoutes clandestines, la manipulation et le rejeu.

Afin de se protéger contre les écoutes et la manipulation, les canaux de communication doivent être chiffrés et signés en utilisant des mécanismes de cryptographie conformes aux recommandations présentes dans le document [RGS_B1].

Le moyen d'identification électronique doit mettre en œuvre des mécanismes de protection contre le rejeu (*par exemple l'inclusion d'un nonce dans le protocole d'échanges des données personnelles*).

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.13 « Sécurité des communications ».

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

3. L'accès à du matériel cryptographique sensible, si ce dernier est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est limité aux rôles et aux applications pour lesquels il est strictement nécessaire. Il convient de s'assurer que ce matériel n'est jamais conservé de manière permanente en texte clair

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés aux points A.9 « Contrôle d'accès », A.10 « Cryptographie » et A.11 « Sécurité physique et environnementale ».

L'accès doit être strictement limité aux seules personnes physiques autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Afin d'assurer la disponibilité des systèmes, il est recommandé que l'accès aux machines soit limité aux seules personnes physiques autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Chaque entité contribuant au schéma d'identification électronique doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante hébergeant le matériel cryptographique avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;

- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;

- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;

- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu.

Plusieurs rôles peuvent être attribués à une même personne physique, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles.

Chaque attribution d'un rôle à un membre du personnel doit lui être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

4. Il existe des procédures permettant de garantir que la sécurité est maintenue sur la durée et qu'il est possible de réagir aux changements des niveaux de risque, incidents et atteintes à la sécurité.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés aux points A.14.2 « Sécurité des processus de développement et d'assistance technique » et A.16 « Gestion des incidents liés à la sécurité de l'information ».

Les changements de nature à affecter la sécurité du moyen d'identification électronique et des systèmes d'information contribuant à la gestion de son cycle de vie ou au processus d'authentification, ainsi que les incidents de sécurité, doivent faire l'objet de notifications à l'ANSSI.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

5. Tous les supports contenant des informations personnelles, cryptographiques ou autres informations sensibles sont stockés, transportés et mis au rebut de façon sécurisée.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.8 « Gestion des actifs ».

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL, ÉLEVÉ

Niveau faible, plus :

Le matériel cryptographique sensible, s'il est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est protégé contre toute manipulation non autorisée.

Le terme « matériel cryptographique sensible » fait référence aux moyens de cryptologie utilisés dans le cadre de la délivrance des moyens d'identification électronique et de l'authentification de l'utilisateur.

La protection des clés cryptographiques que ces matériels manipulent est d'une importance capitale pour la sécurité d'un schéma d'identification électronique.

Les mécanismes dotés d'une protection contre les manipulations non autorisées sont destinés à contrer les tentatives de compromission, de manipulation ou d'usage abusif du matériel cryptographique sensible. Cet objectif est atteint par la mise en œuvre de contrôles de sécurité physiques et logiques pour la protection des clés cryptographiques.

Ces matériels cryptographiques doivent assurer la transparence des mécanismes de sécurité mis en œuvre et satisfaire aux normes de qualité et de sécurité les plus élevées. Les produits doivent être achetés auprès d'un vendeur de confiance et mis en service de sorte à assurer la chaîne de

responsabilité des unités, depuis la fabrication de l'unité jusqu'au lieu de mise en production du module matériel de sécurité.

Pour le niveau de garantie substantiel, la mise en œuvre d'un moyen de cryptologie **qualifié par l'ANSSI au niveau élémentaire du [RGS]** et utilisé conformément aux conditions d'utilisation figurant dans son attestation de qualification, permet d'apporter une présomption de conformité à cette exigence.

Pour le niveau de garantie élevé, la mise en œuvre d'un moyen de cryptologie **qualifié par l'ANSSI au niveau renforcé du [RGS]** et utilisé conformément aux conditions d'utilisation figurant dans son attestation de qualification est obligatoire.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés aux points A.10 « Cryptographie » et A.11 « Sécurité physique et environnementale ».

II.2.4.7. Conformité et audit

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au chapitre 9 « Évaluation des performances » et aux points A.14.2.8 « Test de la sécurité du système » et A.14.2.9 « Test de conformité du système ».

L'ANSSI est chargé de vérifier la conformité aux exigences du présent référentiel. Les décisions de certification de conformité délivrées par l'ANSSI sont validées pour une durée de deux ans. Ces décisions de certification sont délivrées uniquement pour les moyens d'identification électronique visant le niveau de garantie substantiel ou élevé.

Dans le cadre de cette certification, le moyen d'identification électronique est évalué sur pièces et sur place selon le programme de travail défini par le centre d'évaluation et, le cas échéant, par l'Agence nationale de la sécurité des systèmes d'information.

Le fournisseur de moyen d'identification électronique met à la disposition de l'Agence nationale de la sécurité des systèmes d'information et du centre d'évaluation tous les documents nécessaires à l'évaluation. Il leur permet d'accéder à ses locaux, à ses moyens techniques et de rencontrer son personnel.

La charge et le périmètre d'un audit peuvent varier grandement entre les différents niveaux de garantie.

Éléments nécessaires *pour le* niveau de garantie *:* FAIBLE

Il existe des audits internes périodiques dont le champ couvre tous les aspects relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes

Les audits prennent en compte le niveau de risque lié au système/aux éléments du système.

Pour le niveau faible, un audit mené par une équipe interne ou externe permet d'apporter une présomption de conformité à cette exigence.

Un programme d'audit doit être mis en place afin de couvrir l'ensemble du périmètre tous les deux ans.

Il est recommandé de mettre en œuvre un système de gestion de la sécurité de l'information conforme à la norme [ISO_27001], cette exigence étant couverte dans le cadre des contrôles visés au point A.18 « Conformité » (cf. A.18.2 « Revue de la sécurité de l'information »).

Si le moyen d'identification électronique s'appuie sur des certificats électroniques, il est recommandé que l'audit prenne en compte les exigences de la norme [EN_319_411-1], pour le niveau LCP.

Éléments nécessaires *pour le* niveau de garantie *:* SUBSTANTIEL

Il existe des audits internes ou externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.

Les règles du niveau faible s'appliquent.

En complément, pour le niveau substantiel, l'audit doit être mené par :

- un prestataire d'audit de la sécurité des systèmes d'information qualifié au titre du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ; ou

- un organisme disposant d'une accréditation pour la certification de systèmes de management de la sécurité de l'information délivrée par l'instance nationale d'accréditation mentionnée à l'article 1er du décret n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.

L'audit pourra notamment inclure un audit d'architecture, un audit de configuration, un audit de code, des tests d'intrusion et un audit organisationnel et physique

Si le moyen d'identification électronique s'appuie sur des certificats électroniques, il est recommandé que l'audit prenne en compte les exigences de la norme [EN_319_411-1], pour le niveau NCP.

Si l'inscription s'appuie sur un service de vérification d'identité à distance, l'audit doit être mené par un centre d'évaluation répondant aux critères fixés dans le document [EVAL_PVID].

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

1. Il existe des audits externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.

Les règles du niveau faible s'appliquent.

En complément, pour le niveau élevé, l'audit doit être mené par :

- Un prestataire d'audit de la sécurité des systèmes d'information qualifié au titre du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ; ou

- Un organisme disposant d'une accréditation pour la certification de systèmes de management de la sécurité de l'information délivrée par l'instance nationale d'accréditation mentionnée à l'article 1er du décret n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.

Si le moyen d'identification électronique s'appuie sur des certificats électroniques, l'audit doit permettre d'attester du respect de la norme [EN_319_411-1], pour le niveau NCP+.

Éléments nécessaires *pour le* niveau de garantie *:* ÉLEVÉ

2. Lorsqu'un schéma est directement géré par un organisme gouvernemental, il est audité conformément au droit national.

Les règles décrites précédemment s'appliquent également aux schémas gérés par les organismes gouvernementaux.

Annexes

I. Annexe 1 Références documentaires

Renvoi	Document
[CERT_SERV_PVID_CE]	CENTRES D'ÉVALUATION DES SERVICES DE VÉRIFICATION D'IDENTITÉ À DISTANCE - Référentiel d'exigences, version en vigueur Disponible sur https://www.ssi.gouv.fr
[CERT_SERV_PROCESS]	PROCESSUS DE CERTIFICATION D'UN SERVICE – Version en vigueur Disponible sur https://www.ssi.gouv.fr
[eIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE. Disponible sur https://eur-lex.europa.eu
[EN_319_411-1]	ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements Disponible sur : https://www.etsi.org
[ISO_17021]	ISO/IEC 17021 Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences, version en vigueur Disponible sur https://www.iso.org
[ISO_27001]	ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences, version en vigueur Disponible sur https://www.iso.org
[GH]	Guide d'hygiène informatique, version en vigueur. Disponible sur https://www.ssi.gouv.fr/hygiene-informatique/
[CNIL_Guide_conservation]_	Guide pratique –Les durées de conservation, CNIL, version en vigueur. Disponible sur https://www.cnil.fr

Renvoi	Document
[LIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée Disponible sur https://www.legifrance.gouv.fr/
[PVID]	Prestataires de vérification d'identité à distance – Référentiel d'exigences, version en vigueur Disponible sur https://www.ssi.gouv.fr
[QUALIF_PROD]	Processus de qualification d'un produit, version en vigueur. Disponible sur https://www.ssi.gouv.fr/qualification-processus/
[QUALIF_SERV]	Processus de qualification d'un service, version en vigueur. Disponible sur https://www.ssi.gouv.fr/qualification-processus/
[RGPD]	Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. Disponible sur https://eur-lex.europa.eu
[RGS_B1]	Annexe B1 du RGS – Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version en vigueur Disponible sur https://www.ssi.gouv.fr/rgs
[RGS_B3]	Annexe B3 du RGS – Authentification - Règles et recommandations concernant les mécanismes d'authentification, version en vigueur Disponible sur https://www.ssi.gouv.fr/rgs
[SECU_MDP]	Recommandations relatives à l'authentification multifacteur et aux mots de passe – version en vigueur Disponible sur https://www.ssi.gouv.fr/bonnes-pratiques/
[2015/1501]	Règlement d'exécution (UE) 2015/1501 de la commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014. Disponible sur https://eur-lex.europa.eu
[2015/1502]	Règlement d'exécution (UE) 2015/1502 de la commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 Disponible sur https://eur-lex.europa.eu